

**Ex No: 4B**  
**DATE:8/8/24**

## **ANALYSE NETWORK TRAFFIC USING WIRESHARK TOOL**

### **AIM:**

To capture, save, filter and analyze network traffic on TCP / UDP / IP / HTTP / ARP /DHCP /ICMP /DNS using Wireshark Tool

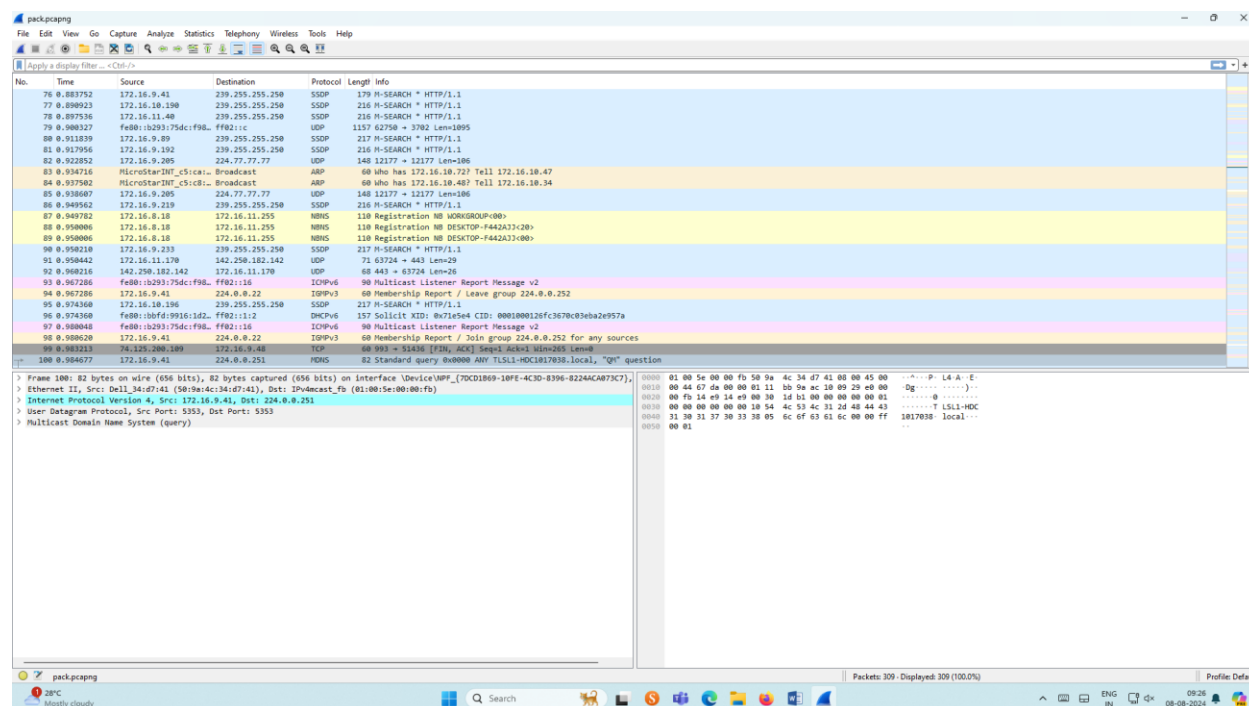
### **Exercises**

#### **1. Capture 100 packets from the Ethernet: IEEE 802.3 LAN Interface and save it.**

### **Procedure**

- Select Local Area Connection in Wireshark.
- Go to capture ☐ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Save the packets.

### **Output**

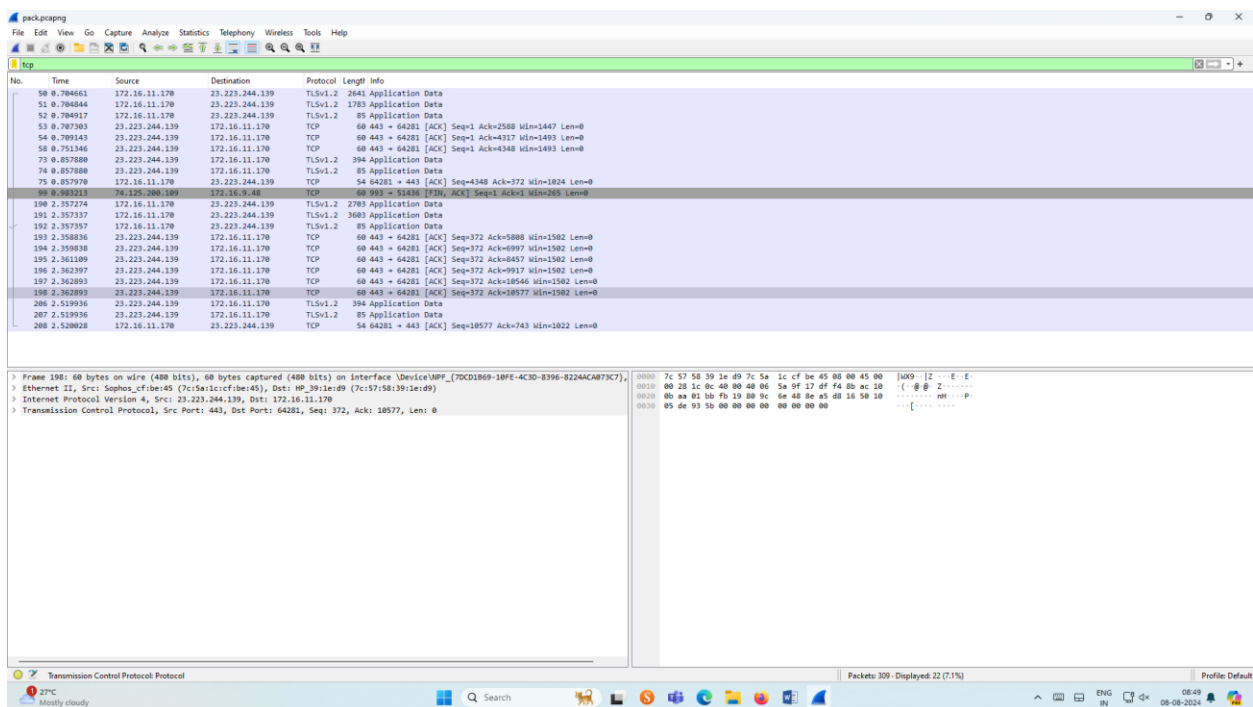


## 2.Create a Filter to display only TCP/UDP packets, inspect the packets and provide the flow graph.

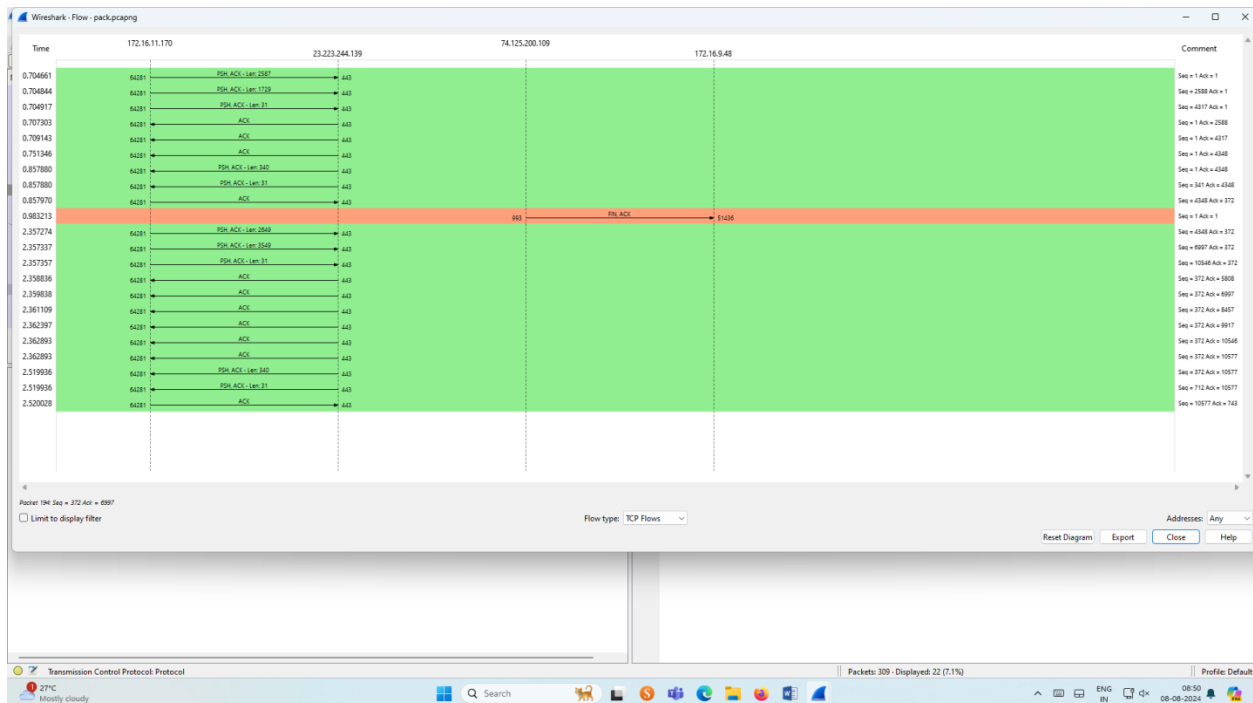
### Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ☐ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search TCP packets in search bar.
- To see flow graph click Statistics ☐ Flow graph.
- Save the packets.

### Output:



### Flow Graph output

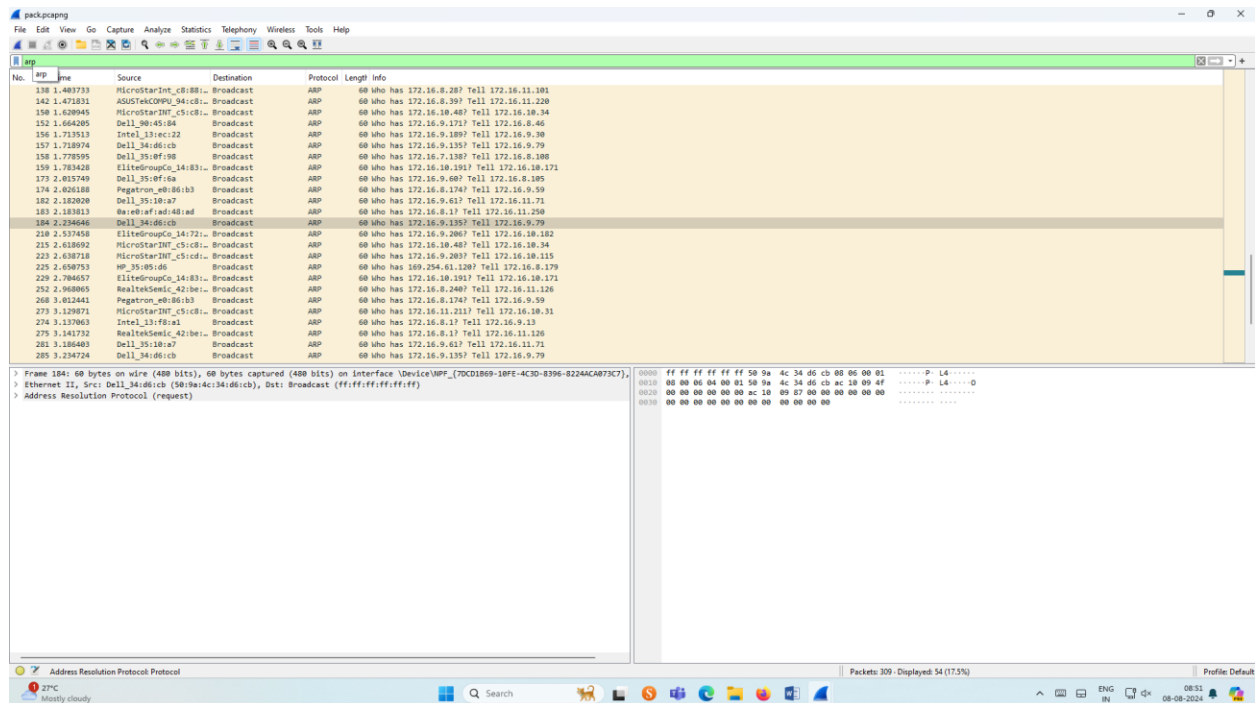


### 3.Create a Filter to display only ARP packets and inspect the packets.

#### Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ☐ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search ARP packets in search bar.
- Save the packets.

#### Output

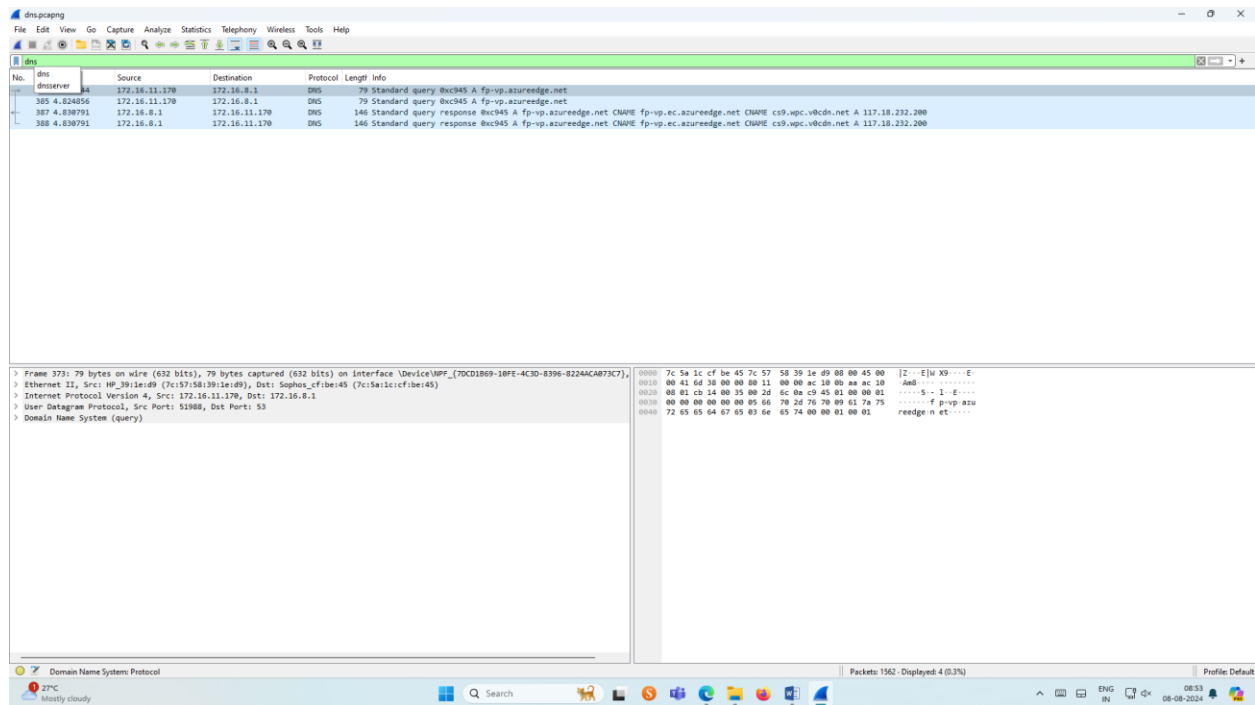


#### 4.Create a Filter to display only DNS packets and provide the flow graph.

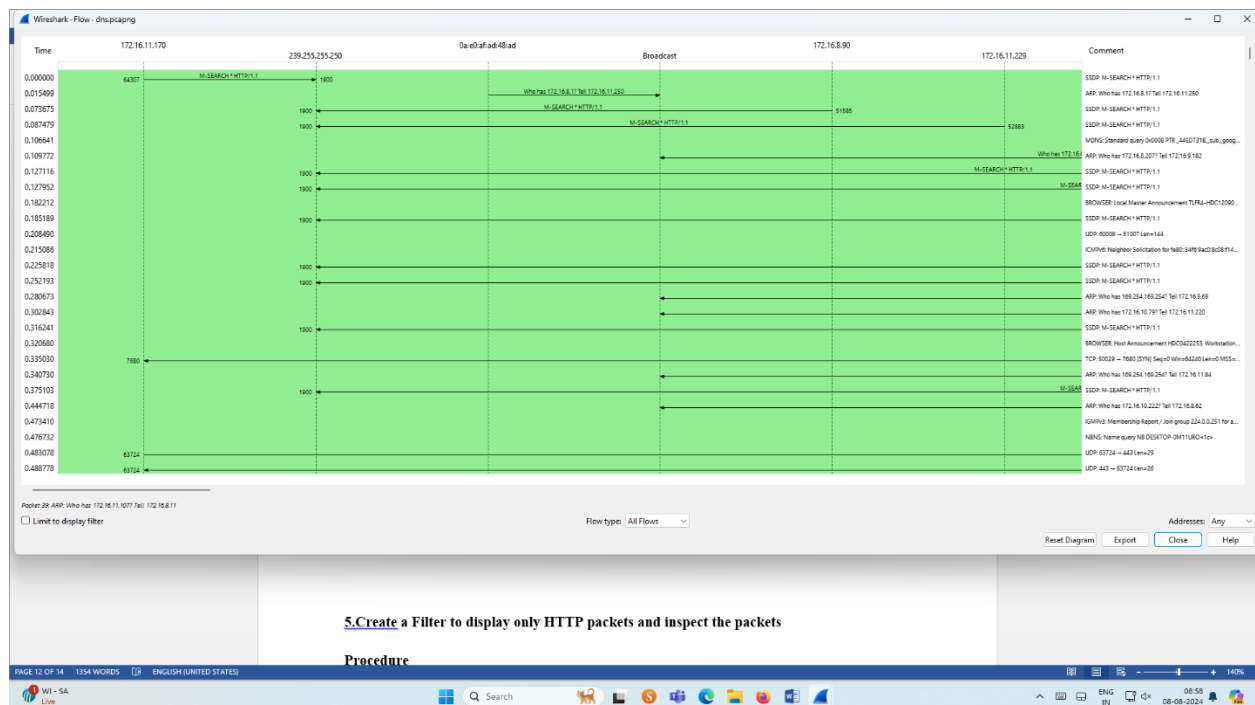
##### Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ☐ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search DNS packets in search bar.
- To see flow graph click Statistics ☐ Flow graph.
- Save the packets.

##### Output



## Graph output

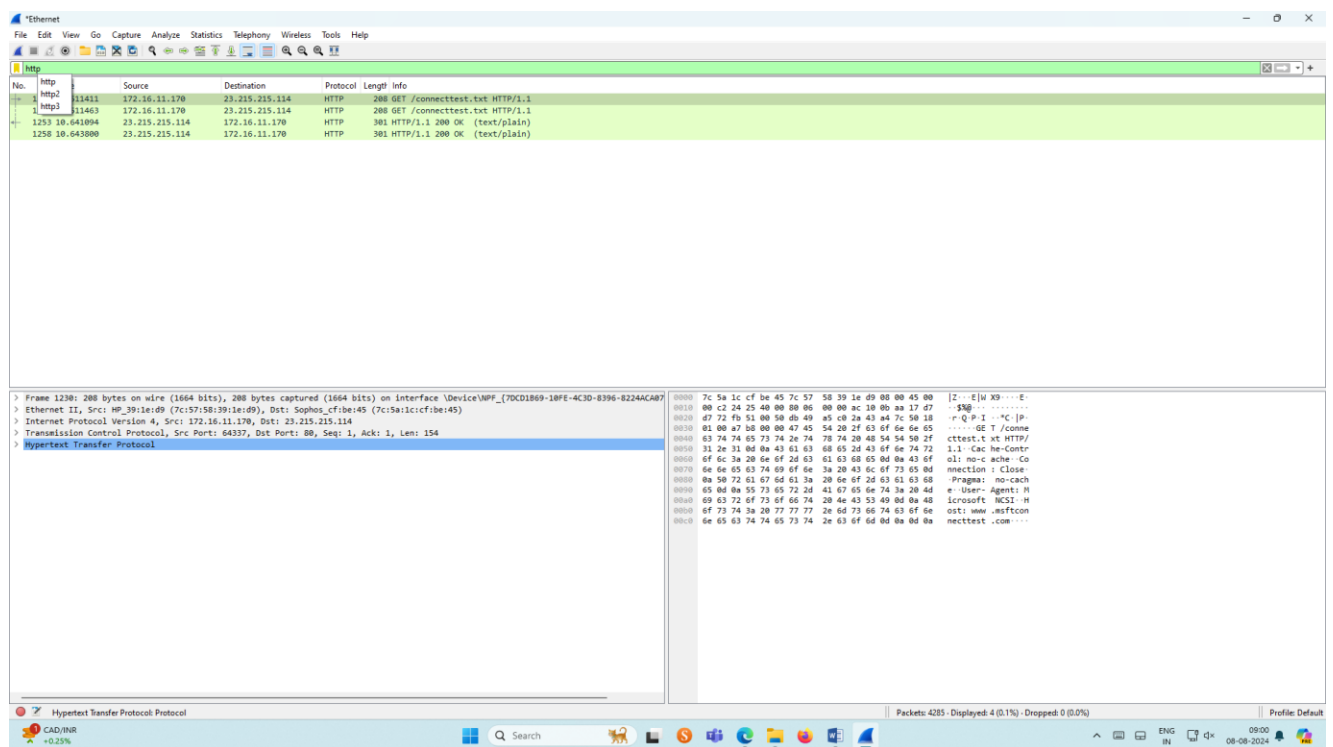


## 5.Create a Filter to display only HTTP packets and inspect the packets

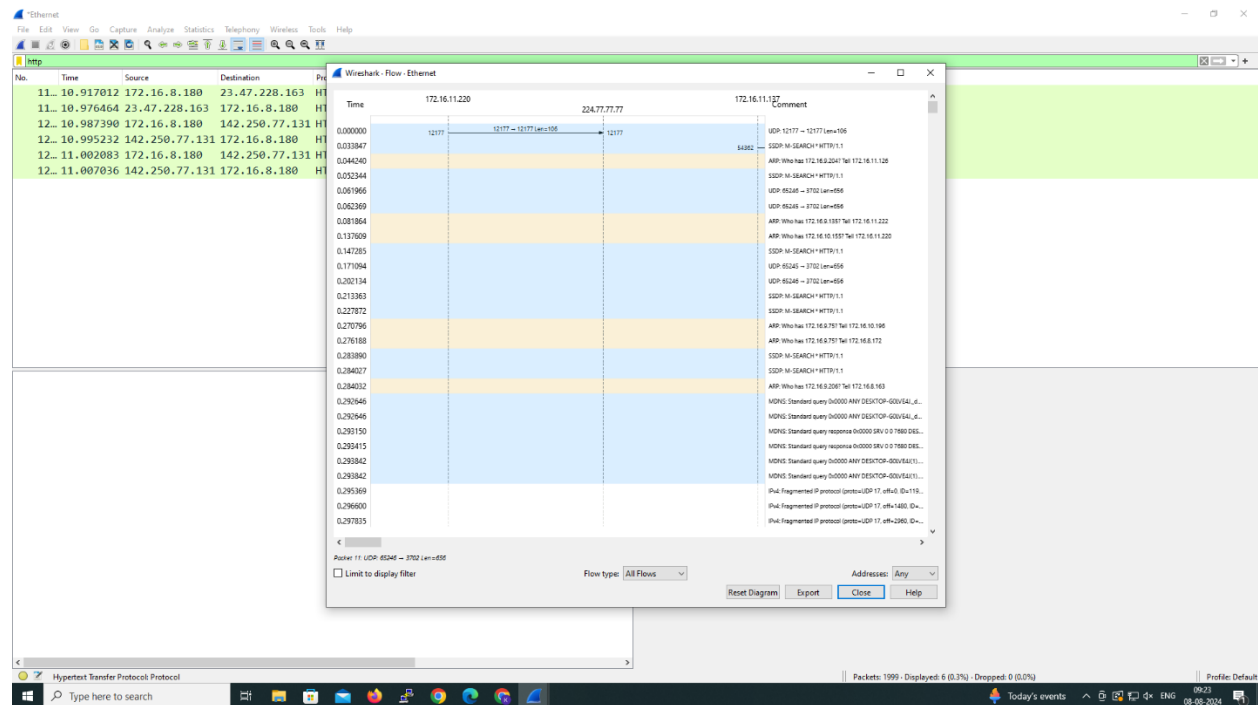
## Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ☐ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search HTTP packets in the search bar.
- Save the packets.

## Output



## Flow Graph output

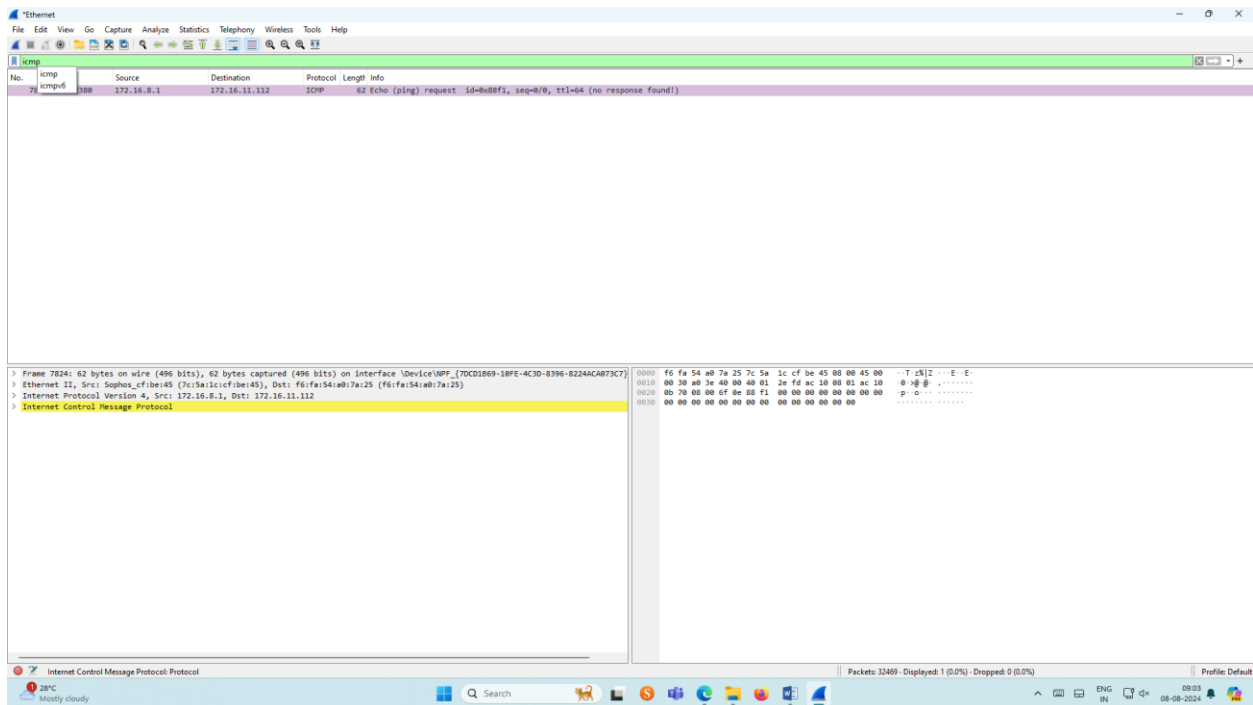


## 6. Create a Filter to display only IP/ICMP packets and inspect the packets.

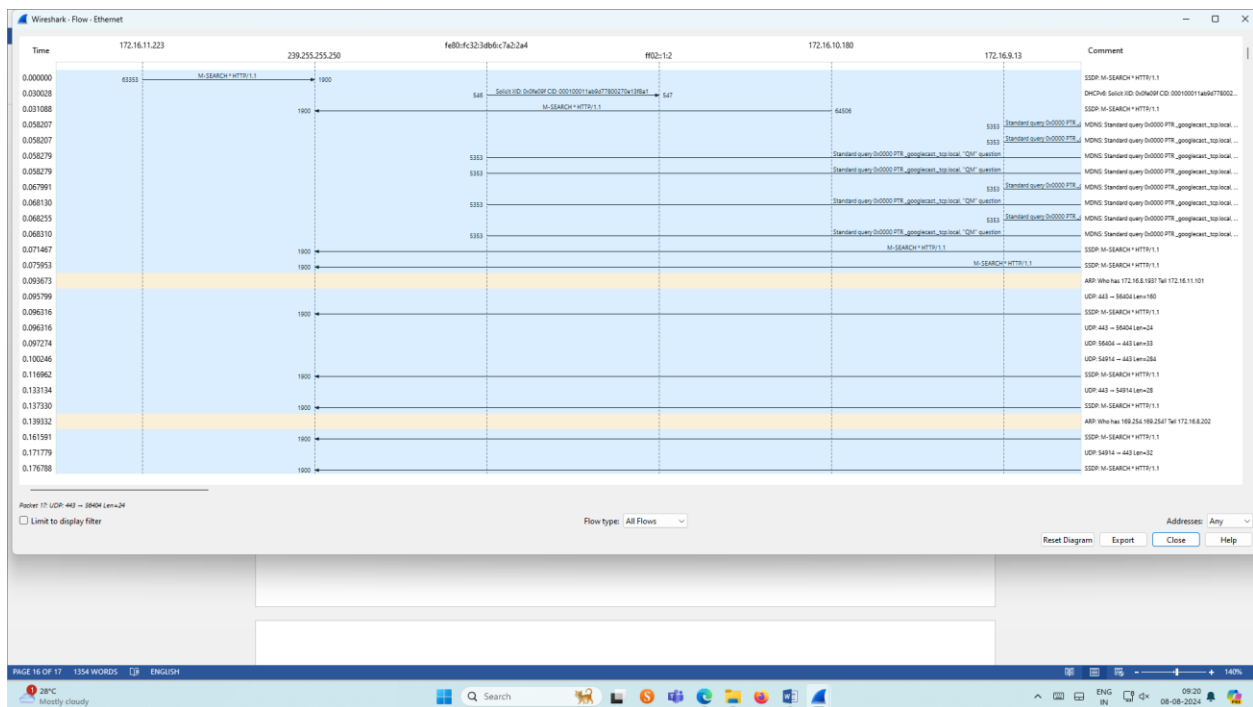
### Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ☐ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search ICMP/IP packets in search bar.
- Save the packets

### Output



## Flow Graph output





## Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ☐ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search DHCP packets in search bar.
- Save the packets

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Meshes, Tools, and Help. Below the menu is a toolbar with icons for file operations, capture control, and analysis tools.

The main window is divided into three panes:

- Packets Pane (Left):** Shows a list of captured packets. Packet 34 is highlighted, which is a DHCP Discover message from 192.168.1.108 to 255.255.255.255.
- Packet Details Pane (Middle):** Provides a hierarchical view of the selected packet's structure. It shows Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Dynamic Host Configuration Protocol (DHCP).
- Packet Bytes Pane (Right):** Displays the raw hexadecimal and ASCII data of the selected packet. The ASCII column shows the DHCP message structure, including magic number, transaction ID, and various flags.

The status bar at the bottom indicates "Dynamic Host Configuration Protocol Request" and shows statistics: Packets: 32469 - Displayed: 18 (0.1%) - Dropped: 0 (0.0%).

The analysing of network traffic using wireshark tool is studied and the output is verified.